Users Do's & Don'ts on Army Networks

Stuart Smith

AMCIO Information Assurance (Corbett Technologies - Millennium Corporation)

ESSENTIAL IN PEACE, INDISPENSABLE IN WAR

References

- AR 25-1, Army Information Management (Feb 02)
- AR 380-19, Information Systems Security (Feb 98)
- AMC Supplement to AR 380-19 (Dec 00)

All of the above documents can be found on the AMC IA Policy Page:

http://www.amc.army.mil/amc/ci/matrix/policy/policy3.htm

AR 25-1- Use of DoD Systems

Use of DoD systems is *"limited to the conduct of official business or other authorized uses."* (Para 6-1,d[1])

"Official business…e-mail messages are…those that are necessary in the interest of the government."

Authorized uses… includes:

- **Brief communications made by…employees while they are traveling on Government business…**
- **Personal communications from the DoD employee's usual work place that are most reasonably made while at the work place**

AR 25-1 – "Authorized" Personal Use

Personal uses are permitted if they:

(a) do not adversely affect the performance of official duties by the employee or the employee's organization.

(b) are of reasonable duration and frequency, and whenever possible, are made during the employee's personal time such as during lunch, break, and other off-duty periods.

(c) are not used for activities related to the operation of a personal business enterprise.

DoD Directive 5500.7-R (JER), Section 2-301 is the basis for Army policy on the use systems. "*Users will abide by these restrictions to prevent security compromises and to avoid disruptions of Army communications systems.*"

AR 25-1 – Other Prohibitions

Users are not permitted to use DoD systems:

- **in a way that would reflect adversely on DoD or the Army**
  - **pornography**
  - **chain e-mail messages**
  - **unofficial advertising**
  - **soliciting or selling via e-mail**
- **unlawful activities, commercial purposes, personal financial gain**
  - **violation of intellectual property**
  - **gambling**
  - **terrorist activities**
  - **sexual or other forms of harassment**

AR 25-1 – Other Prohibitions

- **Political transmissions to include transmissions which advocate the election of particular candidates for public office.**

- **Misuse**
  - **unauthorized entry, use, transfer, and tampering with the accounts and files of others.**
  - **interference with the work of others and with other computing facilities.**

AR 25-1 – Other Prohibitions

- **Interference**
  - **cause, directly or indirectly, congestion, delay, or disruption of service to any computing facilities.**
  - **cause unwarranted or unsolicited interference with others' use of communications.**
  - **Such uses include, but are not limited to:**
    - **chain letters**
    - **Spam**
    - **mail bombs**
    - **unsubstantiated virus warnings**
    - **Broadcast e-mail messages to large groups of e-mail users**

AR 25-1 – Installing Software

Para 6-2, c.3: ***"Users will not install new software packages, software upgrades, free software, freeware, shareware, etc., without the authorization of their systems administrator. Unauthorized software may contain harmful viruses or defects which can result in the loss of data or system failure."***

AR 25-1

Users must be aware of:

- **security issues and their consent to monitoring for all lawful purposes.**
- **restrictions on transmitting classified information over unsecured communications systems.**
- **prohibitions regarding release of access information such as passwords.**
- **the need for care when transmitting other sensitive information.**

AR 380-19 – User Responsibilities

Para 2-11.c.(3) *"When users leave their workstations or personal computers, they will log-off or lock the keyboard and screen until re-authentication."*

2-11.c.(4) Password protected screen savers – 3 to 5 minutes

2-14.e: Users…

- **will safeguard their password**
- **will not disclose their password to unauthorized personnel**
- **will report compromised passwords**

AR 380-19 - User Responsibilities

Users must report all intrusions or suspected intrusions as well as *"suspicious activity"*

B-2: *"Users will employ Internet access for authorized, unclassified U.S. Government business."*

Users are not to use their own private accounts (ie: AOL, Yahoo Mail, personal ISP) for Army-related business unless specifically authorized to do so by their DOIM/DCSIM.

AMC Supplement to AR 380-19

Page 4, paragraph 1-4.

I. ***"…All authorized users of the network must notify the designated IASO upon observation of actions that conflict with the AMC network infrastructure connectivity. Users are responsible for protecting AMC assets, including information systems equipment, data, and information regardless of the security mechanisms that are in place."***

Questions?